UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/480,309	01/10/2000	DAVID N. WILNER	11283/2	4170

30636	7590	05/30/2006		

FAY KAPLUN & MARCIN, LLP
150 BROADWAY, SUITE 702
NEW YORK, NY 10038

EXAMINER
BULLOCK JR, LEWIS ALEXANDER

ART UNIT	PAPER NUMBER
2195	

DATE MAILED: 05/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/480,309	WILNER ET AL.
	Examiner	Art Unit	
	Lewis A. Bullock, Jr.	2195	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>06 March 2006</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-3,5,8-10,13-23 and 25-27</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☒ Claim(s) <u>1-3,5,8-10,13 and 14</u> is/are allowed.

6) ☒ Claim(s) <u>15-23 and 25-27</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   In view of the appeal brief filed on March 6, 2006, PROSECUTION IS HEREBY

REOPENED. The non-final rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed

by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and

appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth

in 37 CFR 41.20 have been increased since they were previously paid, then appellant

must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by

signing below.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 15-18 and 25-27 are rejected under 35 U.S.C. 103(a) as being

unpatentable over "Distributed Operating Systems Based on a Protected Global Virtual

Address Space" by Carter et al.

As to claim 1, CARTER teaches a computer system comprising: a system space (shared space) having a number of memory locations (range of addresses); a number of protection domains, at least one of the number of protection domains owning a portion of the system space (a thread's protection domain controlling a range of addresses), wherein each of the number of protection domains define a set of the number of protection domains to which unprotected access may be made (via a trusted client/server protection domain having both the stub and executable code for directly accessing the other's protection domain) (pg. 1, Introduction, "However, a protection domain in our proposed system corresponds to a set of address ranges in the global address space. Each thread in the system maintains its own view of the global address space, using conventional virtual memory hardware to map portions of the address space into the thread's protection domain. Accesses to protected portions of the global address space would force the accessing thread to change protection domains to the domain associated with the data."; pg. 2, Introduction, "When the client and the server execute within independent address spaces, neither the client nor the server can pass or return pointers to objects within their address space....pg. 2, Protected Global Address Spaces, "Our proposed system supports trusted and untrusted clients, tr4usted and untrusted servers, and data shipping and function shipping invocations. A trusted client or server can directly access anything in the other's protection domain. A trusted client calling a trusted server incurs no overhead beyond a trivial stub executing a single branch instruction. An untrusted client (server) only has access to the parameters (results) and must perform a trap to change protection domains when the client –server

protection boundary is crossed. The stubs for a function shipping invocation are analogous to RPC stubs."; pg. 3, "The example at the bottom of Figure 1 shows that a trusted client's protection domain incorporates the server's protection domain so that the trusted client can access the server data structures directly. Trusted and untrusted servers are handled analogously, which gives the client control over whether or not the server can follow pointers within the client's address space.") It would be obvious to one of ordinary skill in the art that a trusted client protection domain can access multiple trusted server protection domains. However, CARTER does not teach that the view indicates the protection domains and that a protection domain stored in a system space has a kernel and user space. Official Notice is taken in that a protection view is well known in the art to detail the resources a protection view has access of and that a protection domain has both a user and kernel space. Therefore, it would be obvious in view of the teachings of CARTER that the address space of attributed to each protection domain has a system and kernel space and that since Carter details that trusted client and server domains can directly access anything in the other's protection domain due to the incorporation of the others protection domain that the other's protection domain is indicated in its view. The examiner refers Applicant to the numerous cited prior art of record in showing that a kernel and user space of a protection domain is well known in the art (see for instance Wendorf, U.S. Patent 5,845,129).

As to claim 16, CARTER teaches at least one of the protection domains includes at least one of a code module (server code); a link stub (data shipping stubs / function shipping stubs) and an entry point (via a jump instruction) (pg. 2-3, see also figure 1).

As to claims 17 and 18, CARTER teaches the communication between untrusted client / server protection domains wherein the stub performs a trap of changing the protection domain to the recipient domain and executing a jump / branch instruction accordingly to the service code. However, CARTER does not explicitly teach the link stub is part of a linking table referring to a symbol table. It is well known in the art that past implementations of the communication between protection domains involved communication between a linking table to a symbol table. Carter's teachings incorporates both the use of direct communication between protection domains when such domains are trusted and the past approach of trapping a communication between protection domains which involved the use of link tables and symbol tables when such domains are untrusted. Therefore, it would be obvious that CARTER's teachings uses the well known protection domain communication with link tables and symbol tables in order to trap and execute a branch instruction when the client / server is untrusted.

As to claims 25-27, CARTER teaches when the server code and data segment are inaccessible via a faulty modification of the data from the untrusted client's protection domain, the teachings state the stub code must execute a trap to change protection domains to the server's before jumping to the server function (pg. 3).

Therefore, it would be obvious to one of ordinary skill in the art that CARTER teaches

wherein a memory fault is generated (faulty modification) is generated when memory

access is outside the memory range (i.e. inaccessible) and an exception handling

routine that has a protection switch mechanism (i.e. the stub code execute a trap to

change protection domain before jumping to the server function).

4.   Claims 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over

"Distributed Operating Systems Based on a Protected Global Virtual Address Space" by

Carter et al. in view of WENDORF (U.S. Patent 5,845,129).

As to claims 19 and 20, CARTER substantially discloses the invention above.

However, CARTER does not explicitly teach that the protection domain is a system

protection domain.

WENDORF teaches communication between protection domains wherein one

protection domain is a system protection domain that includes at least one code module

including executable code for an operating system service and at least on system object

owned by the system protection domain (col. 3, lines 10-22; col. 9, lines 1-13) and at

least a protection domain list that includes entries for each of the number of protection

domains (col. 5, line 62 – col. 6, line 12). Therefore, it would be obvious to combine the

teachings of CARTER with the teachings of WENDORF in order to facilitate the shared

access of objects within a protection domain among threads such that external access

between protection domains are controlled and delegated (col. 3, lines 1-47).

As to clams 21-23, CARTER teaches at least one of the protection domains is a

first protection domain (client / server) including at least one code module including

executable code; and a number of link stubs (see figure 1); wherein at least one of the

link stubs corresponds to a symbol referenced in the executable code for the first set of

functions (via trapping and jumping to the server code), and such at least one link stub

includes executable code to direct execution to the executable code for services (via a

trusted client executing the server code); wherein the protection domains include a

second protection domain that includes: at least one code module including executable

code for a second set of functions; and a number of entry points; wherein each of the

entry points corresponds to a symbol in the executable code for the second set of

functions; wherein one of the link stubs of the first protection domain correspond to the

entry points in the second protection domain and contains executable code to direct

execution to the one of the entry points in the second protection domain (via using data

shipping stubs to execute a routine o either trap, change context, and jump to the server

code or directly execute the server code) (see figure 1 and pages 2-3) (pg. 1,

Introduction, "However, a protection domain in our proposed system corresponds to a

set of address ranges in the global address space. Each thread in the system

maintains its own view of the global address space, using conventional virtual memory

hardware to map portions of the address space into the thread's protection domain.

Accesses to protected portions of the global address space would force the accessing

thread to change protection domains to the domain associated with the data."; pg. 2,

Introduction, "When the client and the server execute within independent address

spaces, neither the client nor the server can pass or return pointers to objects within their address space....pg. 2, Protected Global Address Spaces, "Our proposed system supports trusted and untrusted clients, tr4usted and untrusted servers, and data shipping and function shipping invocations. A trusted client or server can directly access anything in the other's protection domain. A trusted client calling a trusted server incurs no overhead beyond a trivial stub executing a single branch instruction. An untrusted client (server) only has access to the parameters (results) and must perform a trap to change protection domains when the client –server protection boundary is crossed. The stubs for a function shipping invocation are analogous to RPC stubs.".) However, CARTER does not teach that the protection domain relates to an operating system services. WENDORF teaches communication between protection domains wherein one is a system domain that performs an operating system service.

Allowable Subject Matter

5.   Claims 1-3, 5, 8-10, 13 and 14 are allowed.

6.   The following is a statement of reasons for the indication of allowable subject matter: The cited claims are allowable for at least the following reason: Claim 1 details steps of: determining if the external location is within a second domain that is within a protection view of a first domain, requesting attachment of the second domain to the first domain when the second domain is determined not to be within the protection view of the first domain; and attaching the second domain to the first domain using an attachment mechanism; Claim 8 details step of executing an exception handling routine

in response to the generation of the processing exception, the exception handling

routine including, saving a pre-exception setting of the task protection view, altering in

the task protection view to include a protection view of the second domain, and jumping

to the external location. None of the prior art of record teaches the cited steps. The

publication attributed to Carter et al. teaches attributing an protection domain to another

domain such that the domain has direct access to the data structures and functions of

the connected protection domain when it is determined that both domains are trust-

worthy. However, the cited reference does not detail how such a connection is made.

The cited claims illustrate that this connection either modifies or attaches the protection

view to include the protection view of the second domain. Carter at best teaches a

protection view having an indication of other protection domains. It makes no assertion

as to how the protection view was formed to have this indication. Therefore, the claims

are allowable over the cited prior art of record.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Lewis A. Bullock, Jr. whose telephone number is (571)

272-3759. The examiner can normally be reached on Monday-Friday, 8:30 a.m. - 5:00

p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Meng An can be reached on (571) 272-3756. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

May 24, 2006

LEWIS A. BULLOCK, JR.
PRIMARY EXAMINER

MENG-AI T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100